数理解析研究所講究録
第2055巻 2017年 148-159

G-TYPE NUMBERS OF QUATERNION HERMITIAN LATTICES AND SUPERSINGULAR GEOMETRY.

伊吹山知義（TOMOYOSHI IBUKIYAMA）
大阪大学 (OSAKA UNIVERSITY)

講演では、
（１）５元２次形式の類数と２次４元数的エルミート形式の G-type number との関係、および
（２）超特別アーベル多様体 (superspecial abelian varieties、 つまり超特異楕円曲線の積になっているもの）の偏極で $\mathbb{F}_p$ 上のモデルを持つものの個数、ないしはモジュライ内での主偏極超特異アーベル多様体（つまり超特別アーベル多様体と isogeny なもの）の既約成分で $\mathbb{F}_p$ 上定義されるものの個数の公式と G-type number の関係
について述べた。これらは共に、すでに [7], [8] の論文としてアクセプトされているので、ここでは周辺事情をゆっくり述べることにする。詳しい内容は論文を見ていただくことにしたい。

1. 古典的な結果の復習とその一般化 (1)

標数 p の体上の楕円曲線 E は、p-torsion point が存在しないときに、超特異（supersingular） といわれる。これを最初に取り扱ったのは Deuring [2] であろう。そこでは E の閉体上の同型類は有限個しかないこと、これらはすべて isogeny であること、また $End(E)$ (E の楕円曲線としての閉体上定義された準同形の環）は、p で分岐する $\mathbb{Q}$ 上の四元数環 B の極大整数環であることなどが示されている。B の極大整数環は同型を除いても、一般的には一意的には定まらない。この極大整数環の同型類の個数（あるいは、同じことだが、極大整数環の $B^\times$ 共役類の個数） T を B の type number という。さて、 E の同型類の個数は B の類数 H （つまりある極大整数環の左イデアルを元の左乗法で同値類にわけた個数で、極大整数環の取り方によらない量） に等しいことが知られており、一般論により $T \leq H$ である。E は必ず $\mathbb{F}_{p^2}$ 上定義されたモデルをもつこと（つまり j 不変量が $\mathbb{F}_{p^2}$ に属すること）も知られており、また、E の個数、すなわち B の類数はすでに [4] で知られており、また、そのうち $\mathbb{F}_p$ 上定義されているものの同型類の個数の公式は、最初 [3] で与えられた。その後、後者については [5] で、跡公式でこれを表示することによる別証が与えられていた。これは T の公式が Eichler により具体的に $B^\times$ のアデール化 $B_A^\times$ のヘッケ作用素の跡公式で表示され、また $\mathbb{F}_p$ 上のモデルをもつ E の個数は $2T-H$ で与えられることがわかっていたので、個数も得られたのである。ちなみに、類数と $\mathbb{F}_p$ 上にモデルをもつ E の個数は、$p>2$ では

それぞれ以下の公式で与えられていた。

$$H = \frac{p-1}{12} + \frac{1}{3}\left(1 - \left(\frac{-3}{p}\right)\right) + \frac{1}{4}\left(1 - \left(\frac{-1}{p}\right)\right),$$

$$2T - H = \frac{h(-p) + h(-4p)}{2}$$

ただし $h(-d)$ は $-d$ が 2 次体の判別式の時は、2 次体 $\mathbb{Q}(\sqrt{-d})$ の判別式が $-d$ の（極大とは限らない）整数環の類数、また判別式で無いとき（つまり $-d \equiv 0, 1 \bmod 4$ でないとき）は $h(-d) = 0$ としている。ちなみに、これらの具体的な数値を上げると、

p	2	3	5	7	11	13	17	19	23	29	31	37
H	1	1	1	1	2	1	2	2	3	3	3	3
T	1	1	1	1	2	1	2	2	3	3	3	2

となっており、$p < 37$ では、$H = T$ になっているが、$p = 37$ では、$H = 3, T = 2$ となる。素数が小さいときはすなわち、類数と type number の差が比較的小さい。

さて、次に以上の状況を一般の次元 n のアーベル多様体で考えるとどうなるかについて、少しだけ述べる。

まず p-tortion point を持たないアーベル多様体のクラスはかなり大きくて、少なくとも算術的に取り扱うのに適した最小単位ではない。一方で考えられる一番小さなクラスは、超特異楕円曲線の直積であろう。しかし、超特異楕円曲線 E_i の 2 つ以上の直積 $\prod_{i=1}^{n} E_i$ は皆同型であることが知られている。つまりこのようなものの同型類の個数は 1 である。これは Deligne, Ogus, Shioda による。これは $M_n(B)$ の類数が $n \geq 2$ ならば強近似定理により 1 であることの反映である。よって超特異楕円曲線 E を一つ固定して E^n を考えればたりる。次に小さいクラスは E^n と isogeny なアーベル多様体である。このようなものを超特異アーベル多様体という。一般に（ $n \geq 3$ ならば)、このようなアーベル多様体全体の集合は p-torsion を持たないアーベル多様体の集合よりも小さい。しかし、このようなものの同型類の個数は、主偏極アーベル多様体に限っても無限にある。よって同型類の個数と数えるというのは意味がなく、主偏極アーベル多様体のモジュライの中での軌跡の次元とか、軌跡の既約成分の個数とかが問題になり得る。また 1 変数の時とことなり、偏極の様子が複雑なので、たとえば偏極の degree を固定したときの固定されたアーベル多様体上の偏極の個数とかが問題になり得る。超特異アーベル多様体については、F. Oort 氏を中心に今まで深い研究が行われてきた。私の観点から言えば、総じて言えば、超特異アーベル多様体の幾何学は、四元数的エルミート形式の算術と深い関わりがある、というか極端にいえば、算術理論で全部説明できることが理想であると思う。この意味から言えば、まだまだ開発されていないことは多く、今回の結果はこの方向に付け加える理論の一部である。

2. 4元数的エルミート形式の算術的理論

今回、アーベル多様体について何を新しく得たかという点は後回しにして、話の都合上、4元数的エルミート形式の算術的理論を先に述べる。基礎的な部分は志村の 1963 年の論文 [14] によっている。B を有理数体上の定符号四元数環とし、判別式を D とする。ここで D は $\mathbb{Q}$ の有理素数 q で $B_q = B \otimes_{\mathbb{Q}} \mathbb{Q}_q$ が division になるものの積で、よって D は奇数個の素数の積である。(古典的にはこの D は Grundzahl と呼ばれ、D^2 のことを判別式と呼んでいた。極大整数環の基底から決まる普通の意味での判別式 $\det(Tr(\omega_i\omega_j)) = D^2$ だからである。しかし今では D を判別式と呼ぶことが一般的になっていると思う。) さて、この場合の4元数的エルミート形式の話を書く。

B^n に $(x,y) = \sum_{i=1}^{n} x_i\overline{y_i}$ で正定値4元数的エルミート計量を入れる。ここで $\overline{*}$ は B の main involution を表す。B^n 上の正定値エルミート計量は B 上の基底の変更を除いて、これに一致する。B の極大整数環 O を一つ固定する。B^n 内の lattice L は左 O module の時に O lattice と呼ばれる。$N(L)$ で $\{(x,y); x,y \in L\}$ で生成される両側 O イデアルを表し、これをノルムという。同じノルムを持つ O lattice のうちで極大なものを極大格子という。ここで

$$G = \{g \in M_n(B); gg^* = n(g)1_n, n(g) \in \mathbb{Q}_+^\times\}$$

により代数群 G を定義し、$\mathbb{Q}$ の任意の place v に対して、G_v を G のアデール化 G_A の v 成分とする。$v = \infty$ に対して、$G_\infty^1 = \{g \in G_\infty; n(g) = 1\}$ とするとこれはコンパクトシンプレクティック群 $USp(n)$ である。2つの O lattice L_1, L_2 は, ある $g \in G$ に対して $L_2 = L_1 g$ のとき同じ類に属するといい、任意の有限素点 q に対して $O_q = O \otimes_{\mathbb{Z}} \mathbb{Z}_q$, $L_q = L \otimes_{\mathbb{Z}} Z_q$ と書くことにして、$L_{1,q} = L_{2,q} g_q$ となる $g_q \in G_q$ が存在するときに、同じ種に属するという。同じ種に属する格子全体の集合を種という。ひとつの種 $\mathcal{L}$ の中に含まれる類の個数は有限で、これを $\mathcal{L}$ の類数という。志村 [14] よれば、D の素因子の個数を r とすると、極大格子からなる種は全部で 2^r 個ある。これは $N(L)$ の属する両側イデアルが、有理整数で生成されるイデアルを modulo としてなんであるかで決まっている。たとえば D が素数ならば、種は2つあり、一つは $L = O^n$ を含む種であり、このとき $N(L) = O$ である。もう一つは $N(L) = \mathfrak{P}$ となる L を含む種(ただし $\mathfrak{P}$ は p の上にある O の両側イデアル) である。前者を principal genus といい、後者は特に名前はないが、特に D が素数の時は、principal genus と区別するために区別するために non-principal genus と呼ぶことにする。一般の判別式の場合には、$D = D_1D_2$ (D_i は正の整数) という分解を固定するときに、$q|D_1$ については $N(L_q) = O_q$, $p|D_2$ については $N(L_p) = \mathfrak{P}$ ($\mathfrak{P}$ は p の上にある O の両側イデアル) となるような L が存在し、これらは皆同じ種に属し、これで決まる種を $\mathcal{L}(D_1, D_2)$ と書くことにすれば、これらの 2^r 個の種が maximal lattices で決まる種の全体を与える。さて、$n \geq 2$ ならば、$M_n(B)$ の類数は、強近似定理により 1 である。このことの反映として、任意の B^n の O-lattice は、ある $b \in GL_n(B)$ を用いて $O^n b$ ($b \in M_n(B)$) と書ける。一方で四元数的エルミート行列 h_1, h_2

に対して、ある $\epsilon \in GL_n(O)$ と $a \in \mathbb{Q}^\times$ $a > 0$ があって、$h_2 = a\epsilon^* h_1 \epsilon$ となるとき、h_1, h_2 を同値と呼ぶことにすると、$L = O^n b$ に対して、bb^* という4元数的エルミート行列を対応させることにより、lattice の類と4元数的エルミート行列の同値類は対応がつく。特に L が principal genus に属すると言うことと、4元数的エルミート行列の類の代表が $h \in GL_n(O)$ にとれるということは同値である。一方で、B の判別式が素数 p で $n = 2$ のとき、non-principal genus に対応する4元数的エルミート行列は

$$\begin{pmatrix} pt & r \\ \bar{r} & ps \end{pmatrix} \qquad (t, s \in \mathbb{Z}, r \in \mathfrak{P}, p^2ts - r\bar{r} = p)$$

ととれる。

3. G-TYPE NUMBER OF QUATERNION HERMITIAN LATTICES

さて、$n \geq 2$ では、$M_n(B)$ の類数が1であることの反映として、$M_n(B)$ の極大整数環は同型を除いて一意的に定まる。この意味では $M_n(B)$ の type number は1である。しかし、これ以外に4元数的エルミート計量に関係して、G-type number というものを定義することができる。以下 $n \geq 2$ と仮定しておく。$\mathcal{L}$ を B^n 内の種として、類数を $h = H(\mathcal{L})$, 類の代表を $L_1, \ldots, L_h$ とする。 このとき、$L_i = O^n b_i$ の右 order つまり

$$R_i = \{b \in M_n(B); L_i b \subset L_i\} = b_i^{-1} M_n(O) b_i$$

はもちろん maximal order である。$g \in G$ に対して、L_i と同じ類に属する格子 $L_i g$ $(g \in G)$ の右 order は $g^{-1} R_i g$ であるが、このような R_i と $g^{-1} R_i g$ を同一視することが考えられる。つまり $\{L_1 \ldots, L_h\}$ の右 order $\{R_1, \ldots, R_h\}$ を G 共役で同値類にわけた代表の個数を $\mathcal{L}$ の G-type number と呼ぶことにして $T(\mathcal{L})$ とかく。このような量は [6] (I) で導入したのが最初である。あきらかに $T(\mathcal{L}) \leq H(\mathcal{L})$ である。類数 $H(\mathcal{L})$ の公式は原理的には跡公式で求めることができる。すなわち、これは $L \in \mathcal{L}$ の固定群できまる G_A の部分群についての保型形式の次元であって、これはヘッケ作用素 $T(1)$ の跡であり、一般論としては、G 共役類にわたる、ある種の量の和で表示されるのはよく知られている。もちろん実際の計算は面倒である。たとえば、$n = 2$ のときの、maximal lattices の genus すべてについては、[6] に具体的な公式が与えられている。一方、$T(\mathcal{L})$ については、たとえば [6] (I) に、ほとんど証明無しで、いくつかのヘッケ作用素の跡の線形結合で与えられるという結果を、principal genus について述べた。（昔の論文では、類数公式のあとのリマークという趣があったので、あまり詳しく述べなかったが、今回の論文 [8] ではもっと一般の場合に詳しく証明を書いてある。）また具体的な明示公式は $n = 2$ のときは、[10] に述べてある。ここでは、一般の $T(\mathcal{L})$ のヘッケ作用素による公式を定理としてあげておく。基礎体が任意の場合にも拡張できるのだが、ここでは基礎体が $\mathbb{Q}$ の場合だけのべておく。まずヘッケ作用素について説明する。L を

maximal lattice として、$\mathbb{Q}$ の有限素点 q について

$$U_q(L) = \{g_q \in G_q; L_q g_q \subset L_q\}$$

とおく。また $U = U(L) = G_\infty \prod_q U(L_q)$ とおく。ここで $U(L)\backslash G_A/G$ 上の $\mathbb{C}$ 値関数の空間を

$$\mathfrak{M}_0(U(L)) = \{f : G_A \to \mathbb{C}; f(uga) = f(g), u \in U(L), a \in G\}$$

とおく。これはベクトル空間として $\mathbb{C}^h$ と同型だが、つまりは $U(L)$ に関するウェイトが 0 の保型形式の空間である。$\mathfrak{M}_0(U(L))$ への double coset UzU の作用を次のように定める。$f(g) \in \mathfrak{M}_0(U(L))$, $UzU = \cup_{i=1}^d z_i U$ とするとき、

$$([UzU]f)(g0 = \sum_{i=1}^d f(z_i^{-1}g) \qquad (g \in G_A).$$

また、各 $q|D$ に対して、$R_q = \{\alpha \in M_n(B_q); L_q\alpha \subset L_q\}$ とおくとき、$\omega_q \in R_q \cap G_q$ かつ $\omega_v^2 = -p$ かつ $R_q\omega_q = \omega_q R_q$ となる元が存在することが示せる。このとき、各 D の約数 $0 < m|D$ に対して、$omega(m) = (g_v) \in G_A$ を v がアルキメデス的、または $v \nmid m$ のときは $g_v = 1_n$, $v|m$ の時は $g_v = \omega_v$ として定めることにする。$R(m) = U\omega(m)U$ とおく。このとき $R(m) = U\omega(m)$ でもある。

Theorem 3.1. $D = p_1 \cdots p_r$ とするとき、次の公式が成り立つ。

$$T(\mathcal{L}) = \frac{1}{2^r} \sum_{m|D} Tr(R(m))).$$

ここで $Tr(R(m))$ は $R(m)$ の $\mathfrak{M}_0(U(L))$ への作用の跡という意味である。たとえば　$D = p$ （素数）ならば $r = 1$ であり、$Tr(T(1)) = H(\mathcal{L})$ （類数）であるから、

$$2T(\mathcal{L}) - H(\mathcal{L}) = Tr(R(p))$$

である。

4. Quinary lattice と $n = 2$ の G-type number

たとえば $USp(1)/\{\pm1\} \cong SO(3)$ であるから、3 元 2 次形式と 4 元数環には何か関係があることが想定されるし、またそういう論文もある。そこで $n = 2$ とすると、$USp(2)/\{\pm1\} \cong SO(5)$ であるから、5 元 2 次形式と 4 元数的エルミート格子にはなにか関係があることが考えられる。実際、たとえば [6](I) の最後の方で、principal genus の G-type number がある種の 5 元 2 次形式の類数と等しいことを述べてある。(証明はほとんど省略してあるが。) この結果は任意の maximal lattice の genus に拡張することができる。大雑把に言って、任意の分割 $D = D_1D_2$ について $T(\mathcal{L}(D_1, D_2))$ はある種の 5 元 2 次形式の類数に等しい。(詳しい証明は [7] を参照。) ただし話が少々複雑になるのをさけるために、以下 D は奇数と仮定する。任意の maximal とは限らぬ genus についてどうなるかについては考えたことがないが、一般にこういう算術的対応を正確に述べるのは、それほど易しいわけではないと

思われる。さて、以上で maximal lattices に対応するものが、どのような2次形式なのかを、もっと具体的に説明する。W を $\mathbb{Q}$ 上5次元のベクトル空間とし、W 上の2次形式 Q に関する even Clifford algebra $C_2(W)$ が与えられた $\mathbb{Q}$ 上の定符号4元数環 $B=\mathbb{Q}+\mathbb{Q}\alpha+\mathbb{Q}\beta+\mathbb{Q}\alpha\beta$ (ただし $\alpha^2=-a_1$, $\beta^2=-a_2$, $\alpha\beta=-\beta\alpha$, a_1, $a_2>0$) に関して、$M_2(B)$ と同型になるようなものを考えたい。じつはこのような2次形式 Q は similarlity class の違いをのぞき、W の基底 $e_1, e_2, \ldots, e_5$ について $Q(e_1)=Q(e_2)=1$, $Q(e_3)=a_1$, $Q(e_4)=a_4$, $Q(e_5)=a_1a_2$ $(a_1, a_2>0)$ となるものに限る。実際に、このとき、$\alpha=(e_4e_5)/a_2$, $\beta=(e_3e_5)/a_1$ と置き、$C_0=\mathbb{Q}+\mathbb{Q}e_1e_2+\mathbb{Q}e_2e_3e_4e_5+\mathbb{Q}e_1e_3e_4e_5$ とおけば、自然に $C_0\cong M_2(\mathbb{Q})$ であり、 $C_0(W)=B\otimes C_0=M_2(B)$ となる。Clifford algebra は $e_{i_1}\cdots e_{i_r}\to e_{i_r}\cdots e_{i_1}$ で決まる involution を持つが、これは $M_2(B)$ 上で $g\to g^*$ を引き起こす。さて、W の元は Clifford algbra 全体 $C(W)$ の中では degree 1 の部分であるから、$C_0(W)$ には、入らないけれど $e_1e_2e_3e_4e_5$ が $C(W)$ の中心の元であるから、$V=e_1e_2e_3e_4e_5W\subset C_0(W)$ を考えると、$C_0(W)$ の元と W の元の積が自然に V の元との積に移る。ここで

$$V=\left\{\begin{pmatrix} t & r \\ \bar{r} & -t\end{pmatrix}; t\in\mathbb{Q}, \in B\right\}$$

となる。定義により even Clifford group Γ_2 というのは $g\in C_2(W)^\times$ であって、$g^{-1}Wg\subset W$ となる元のことであるが、これは $g^{-1}vg\in V$ がすべての $v\in V$ について成り立つ元と言っても同じことである。しかし $g\in\Gamma$ については、$gg^*\in\mathbb{Q}$ であることが知られている。これは $g\in G$ ということであり、一方 $v\in V$ かつ $g\in G$ ならば、$g^{-1}vg=n(g)g^*vg$ であり、上の V の表示からこれは4元数的エルミート対称行列であり、Trace=0 はあきらかだから $g^{-1}vg\in V$ である。すなわち $\Gamma_2=G$ である。もちろんこれはよく知られている。$v\to g^{-1}vg$ は V の metric を変えず、G から $SO(V)$ への準同形を引き起こす。(これは Q のその定数倍に変えても同じである。) このとき $G/\mathbb{Q}^\times\cong SO(V)$ がよく知られている。ただし $\mathbb{Q}^\times$ は $\{c1_2; c\in\mathbb{Q}^\times\}$ と同一視している。よって大雑把に言って lattice の右 order の G 共役類が、5元2次形式の格子の同値類と対応しそうだというのはわかる。しかしこれを精密に見る必要がある。

さて、以上のように $V=\mathbb{Q}+B$ と同一視して,2次形式は $Q(t,r)=t^2+N(r)$ $(t\in\mathbb{Q}, r\in B)$ と考えてもよい。都合上ここで2次形式を少し similarlity class のなかで変更する。積への分割 $D=D_1D_2$ $(D_i>0)$ を固定して、 $Q(t,r)=(t^2+N(r))/D_2$ とする。この2次形式の判別式は $\mathbb{Q}$ 上 mod $\mathbb{Q}^{\times 2}$ で決まるが、これは $2D_2$ となる。さて、分割 $D=D_1D_2$ に応じて、2次形式の種を決めたい。この2次形式の変更は、もちろん Clifford algebra などには何も影響しない。2次形式の種を定義するために、局所的な格子をまず定義する。B の極大整数環 O を一つ固定しておく。まず素数 q が $q\nmid D_2$ を満たすとき、

$$M_q=\left\{\begin{pmatrix} t & r \\ \bar{r} & -t\end{pmatrix}; t\in\mathbb{Z}_q, r\in O_q\right\}.$$

とおく。$q|D_2$ の時は、これよりは複雑である。群と格子の表示を簡単にするために少し座標変換する必要がある。$\xi_v \in GL_2(O_q)$ で $\xi_q\xi_q^* = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ となる元が存在する。ここで $G_q^* = \xi_q G_v \xi_q^{-1}$, $V_q^* = \xi_q V_q \xi_q^{-1}$ とおくと、$g \in G_q^*$ は V_q^* 上の $v \to gvg^{-1}$ として作用する。$B_q^0 = \{b \in B_q; Tr(b) = 0\}$ とおくと、

$$V_q^* = \left\{ \begin{pmatrix} y & t \\ s & -y \end{pmatrix}; t, s \in \mathbb{Q}_q, y \in B_q^0 \right\}$$

となる。π を O_q の素元として、V_q^* の格子を

$$K_q = \left\{ \begin{pmatrix} y & t \\ s & -y \end{pmatrix} \in V_q^*; t, s \in \mathbb{Z}_q, y \in \pi O_q \cap B_q^0 \right\}$$

で定義する。これらの記号の準備のもとに、V 内の格子の集合 $\mathcal{M}(D_1, D_2)$ を次のように決める。$M_0 \subset V$ は ($\mathbb{Z}$ 上の）格子で、任意の素数 q に対して、$M_0 \otimes_{\mathbb{Z}} \mathbb{Z}_q$ は
(1) $q \nmid D_2$ ならば上記の M_p を G_q 共役
(2) $q \mid D_2$ ならば、上記の K_p について $\xi_1^{-1} K_q \xi_q$ と G_q 共役
となるような集合。この集合が空集合でないことはすぐわかるので、もちろん $G_q \to SO(V_q)$ は surjective だから、これは 2 次形式の意味での $SO(V)$ に関する種であるが、今次数は 5 であり、$O(V)/SO(V) = \{\pm id.\}$ であるから、$SO(V)$ に関する種や類数は、$O(V)$ に関する種や類数と同じものである。

Theorem 4.1. *$D = D_1D_2$ $(D_i > 0)$ とするとき、極大格子の種 $\mathcal{L}(D_1, D_2)$ の G-type number と 5 元 2 次形式の種 $\mathcal{M}(D_1, D_2)$ の類数 $H(\mathcal{M}(D_1, D_2))$ は等しい。すなわち、次を得る。*

$$T(\mathcal{L}(D_1, D_2)) = H(\mathcal{M}(D_1, D_2)).$$

ちなみに、このような 2 次形式の判別式は $2D_1^2D_2$ であることがわかり、また 2 では局所的に

$$(2D_2) \perp \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \perp \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

と同型なことがわかる。このような 2 次形式の類数は [1] に具体的な公式が完全に与えられており、よって別にヘッケ作用素の跡を計算するまでも無く、浅井照明氏の結果を流用すれば、G-type number がわかることになる。$D = D_1 = p$ の時の具体的な結果は、[10] に応用があげてある。あとで $D = D_2 = p$ のときは、具体的に述べる。

5. 幾何学の復習とその一般化 (2)

アーベル多様体 A に対して、A^t を A の dual ($= Pic^0(A)$) とするとき、A の effective divisor D に対して、A から A^t の isogeny を $\phi_D(t) = Cl(D_t - D) \in A^t$ と定義する。ここで Cl は A の因子の linear equivalence class を、また D_t は D を t で平行移動した因子を表す。A から A^t への isogeny λ であって、ある effective divisor D に対し

て、$\lambda=\phi_D$ となるとき、λ を偏極と呼ぶ。λ が同型の時 λ を主偏極という。これは D の n 重 intersection が $n!$ であることと同値である。特に偏極 λ_1, λ_2 は $\alpha \in Aut(A)$ で $\lambda_2=\alpha^t\lambda_1\alpha$ となるものがあるとき同値であるという。ただし α^t は α の dual であり、$End(A^t)$ の元である。

以下、E を超特異楕円曲線で、$\pi \in End(E)$ で $\pi^2=-p$ の元が存在するようなものとする。このような超特異楕円曲線は存在することが知られているので、これを固定しておく。(極大整数環 $O=End(E)$ の条件でいえば、p 上の両側イデアル $\mathfrak{P}$ が単項であるようなものである。) $End(E)\otimes_{\mathbb{Z}}\mathbb{Q}=B$ とおき、B の判別式を p とする。B の main involution を $\overline{*}$ とかく。E^n の divisor X を

$$X=\{0\}\times E^{n-1}+E\times\{0\}\times E^{n-2}+\cdots+E^{n-1}\times\{0\}$$

と置くと、$X^n=n!$ が容易にわかるので、ϕ_X は同型である。$End(E)\otimes_{\mathbb{Z}}\mathbb{Q}=B$ として、$g=(g_{ij})\in M_n(B)$ に対して、$g^*=(\overline{g_{ij}})$ と書く。このとき、任意の偏極 λ に対して、$h=\phi_X^{-1}\lambda$ とおけば、もちろん $h\in End(E^n)$ だが、このとき $h^*=h$ であり、またこれは正定値になるのはアーベル多様体の一般論である。(実際には任意の $\alpha\in End(E^n)$ に対して、$\alpha^*=\phi_X^{-1}\alpha^t\phi_X$ である。) 言葉を流用して h も E^n の偏極と呼んでもそう間違いはおこらないであろう。h と同値な偏極は、$End(E^n)$ の中で考えれば

$$\phi_X^{-1}\alpha^t\lambda\alpha=\phi_X^{-1}\alpha^t\phi_X\phi_X^{-1}\lambda\alpha=\alpha^*h\alpha$$

であるから 4 元数的エルミート行列 h を $GL_n(O)=M_n(O)^\times$ で挟んだ同値類が偏極の同値類である。たとえば $Hm(h)=1$ (Hm はジョルダン代数のいわゆる Haupt Norm、つまり det の代わりを務めるもの) なる $h\in M_n(O)$ 全体は前の節などで述べた 4 元数的エルミート格子の principal genus (主種) と対応しているのはかなり容易にわかる。実際上、principal genus の類数が E^n 上の主偏極の同値類の個数である。(これは実際は $n=1$ でも正しい、この場合は類数も主偏極の個数も 1 で、面白くないが。) また、[11] ないしは [12] によれば、n 次元の主偏極アーベル多様体のモジュライ全体の中での主偏極超特異アーベル多様体の軌跡は一般に既約ではなく、その既約成分の個数は、n が偶数ならば B^n の non-principal genus の類数 $H(\mathcal{L}(1,p))$ に等しく、n が奇数ならば principal genus $H(\mathcal{L}(p,1))$ の類数に等しいことが知られている。ここで superspecial と supersingular の絡み具合とか、あるいは一般の次元の低い部分の交差の様子とかいろいろ算術が入り込む余地があり、わかっている部分もいろいろあるが、まだ十分とはいえない。これらは基本的に全部代数閉体上の話である。

そて、今回述べたいのは、定義体との関係である。すなわち古典的な結果で言えば $j\in\mathbb{F}_p$ となる超特異楕円曲線の個数の勘定に当たる部分が一般にどうなるかである。

さて、E を前の通りとして、E^n の偏極は、$End(E^n)$ の元がすべて $\mathbb{F}_p^2$ で定義されるのだから、偏極も $\mathbb{F}_p^2$ 定義されている。少し話が微妙なので、あえてきちんと定義しておくと、E^n 上の偏極 λ が体 k 上で定義されるというのは、(E^n,λ) が k 上のモデルをもつこと、つまり

k 上定義されたアーベル多様体 A と A 上の偏極 μ が存在して、μ が k 上で定義され、かつ (E^n, λ) と (A, μ) が k を含む閉体上で同型という意味とする。これは偏極 λ が k 上定義されるというのとはもちろん意味が違う。 A と E^n は k 上同型かどうかはわからないからである。いずれにせよ、偏極超特別アーベル多様体 (E^n, λ) は $\mathbb{F}_{p^2}$ 上のモデルを持つのは明らかである。よって、$\mathbb{F}_p$ 上のモデルを持つかどうかが問題になる。さて、たとえば (E^2, λ) が $\mathbb{F}_p$ 上のモデルをもつようなものの個数を数えることを考えてみよう。この場合、λ は $End(E^n)$ の元と $\phi_X^{-1}\lambda$ で同一視すれば、この 4 元数的エルミート行列の属する種というのが考えられる。これは $bb^* = \phi_x^{-1}\lambda$ $(b \in GL_n(B))$ と書いたとき O lattice $O^n b$ の属する（4 元数的エルミート計量の意味での）種といっても同じことである。この種を $\mathcal{L}(\lambda)$ と書くことにする。一方で、$\phi_X^{-1}\lambda \in \mathcal{L}(\lambda)$ となる λ の全体を $\mathcal{P}(\lambda)$ と書くことにしよう。また, $\mathcal{L}(\lambda)$ の類数と G-type number をそれぞれ $H(\lambda), T(\lambda)$ と書くことにする。、

Theorem 5.1. E を超特異楕円曲線とする。E^n の偏極 λ をひとつ固定する。このとき、偏極アーベル多様体 (E^n, μ), $(\mu \in \mathcal{P}(\lambda))$ の閉体上の同型類の個数は $H(\mathcal{P}(\lambda))$ と等しい。またこのような偏極アーベル多様体のうちで、$\mathbb{F}_p$ 上定義されるモデルを持つものの個数は $2T(\mathcal{L}(\lambda)) - H(\mathcal{L}(\lambda))$ に等しい。

証明は、論文 [8] を参照されたい。

さて、以上の結果は、応用がある。まず、直接的な応用から述べると、$n = 2$ ならば E^2 の主偏極（を決める divisor class) は、楕円曲線の直和か、または種数 2 の代数曲線 C かのどちらかである。このとき、C のヤコービ多様体 $J(C)$ は E^2 と同型になる。主偏極 C が $\mathbb{F}_p$ 上定義されるというのは、C が $\mathbb{F}_p$ 上のモデルを持ち、$J(C) \cong E^2$ となると言うことである。このような曲線の (閉体上の同型類の）個数が principal genus の G type number と類数でカウントされていることになる。（もちろん既約でないものを計算して除いておく必要がある。）この結果については、[10] に述べてあるとおりだが、かなり昔の結果なので、ここでは繰り返さない。

ここで、さらに主偏極超特異アーベル多様体のモジュライに応用がある。まず、n 次元の主偏極アーベル多様体全体のモジュライ $\mathcal{A}_{n,1}$ の中での主偏極超特異アーベル多様体 (A, λ) の軌跡 $\mathcal{S}_{n,1}$ を考える。ここで A が超特異というのは E^n と isogeny という意味であった。（もし超特別 (つまり A が E^n と同型）のもののみ考えると、主偏極の個数は有限なので、モジュライの中ではこのようなものは、つまり 0 次元の点の集合にしかならない。）さて、この軌跡全体は $\mathbb{F}_{p^2}$ 上定義されている。しかしこれは既約では無く、各既約成分も $\mathbb{F}_{p^2}$ 上定義されている。このうちで $\mathbb{F}_p$ 上のモデルをもつものの個数がわかる。今 $\mathcal{L}_{pr}$ で B^n の principal genus を、また $\mathcal{L}_{npr}$ での non-principal genus を表すとすると、次を得る。

Theorem 5.2. 上記の軌跡 $\mathcal{S}_{n,1}$ の既約成分で $\mathbb{F}_p$ 上のモデルをもつものの個数は、n が偶数ならば $2T(\mathcal{L}_{npr}) - H(\mathcal{L}_{npr})$, また n が奇数ならば、$2T(\mathcal{L}_{pr}) - H(\mathcal{L}_{pr})$ である。

伊吹山知義（TOMOYOSHI IBUKIYAMA） 大阪大学 (OSAKA UNIVERSITY)

証明はやはり [8] を参照されたい。

Corollary 5.3. 任意の $n \geq 2$ と標数 p に対して、$\mathcal{S}_{n,1}$ は $\mathbb{F}_p$ 上のモデルを持つ既約成分が存在する。また $n=2$ で $p<167$ ならば、任意の既約成分は $\mathbb{F}_p$ 上定義されている。

証明の方針は $n=2$ で $\mathbb{F}_p$ 上のモデルを持つものがあることを言うことにある。一般の場合は単にそれらに対応する 4 元数的エルミート格子の直和をとれば、n が偶数で対応する偏極が $\mathbb{F}_p$ 上のモデルを持つことがわかる。n が奇数の時は、O^n はいつでも $\mathbb{F}_p$ 上のモデルをもつ主偏極に対応するので、明らかである。

参考のために、$n=2$ の時、$\mathcal{L}_{npr}$ に関する類数と G -type number の数値の公式と小さい p に対する具体的な数値をあげておく。標数 p によるので、$T(1,p)=T(\mathcal{L}_{npr})$, $H(1,p)=H(\mathcal{L}_{npr})$ と書くことにする。($(1,p)$ と書いているのは、判別式 $p=D_1D_2$ という分解で、$D_1=1$, $D_2=p$ という意味である。) このうち類数は [6] (II) からの引用であり、また G-type number は、前に述べたように 5 元 2 次形式の類数と等しく、この値は [1] からの引用である。

Theorem 5.4. $p=2,\ 3,\ 5$ については $T(1,2)=T(1,3)=T(1,5)=1$ である。素数 $p\geq 7$ が $p\equiv 1 \bmod 4$ のときは

$$\begin{aligned}
T(1,p) \;=\; & \frac{p^2-1}{2^7 3^2 5}+\frac{1}{2^6\cdot 3}\left(9-2\left(\frac{2}{p}\right)\right)B_{2,\chi}+\frac{1}{2^5}h(\sqrt{-p})+\frac{1}{2^4}h(\sqrt{-2p}) \\
& +\frac{1}{2^3\cdot 3}\left(3+\left(\frac{2}{p}\right)\right)h(\sqrt{-3p})+\frac{5}{2^6\cdot 3}(p-1) \\
& +\frac{1}{2^4}\left(1-\left(\frac{2}{p}\right)\right)+\frac{1}{2^4 3^2}\left(p-\left(\frac{-3}{p}\right)\right)\left(3+\left(\frac{-3}{p}\right)\right) \\
& +\frac{1}{2^3 3}\left(1-\left(\frac{-3}{p}\right)\right)+\frac{1}{2\cdot 5}\left(1-\left(\frac{p}{5}\right)\right).
\end{aligned}$$

また素数 $p\geq 7$ が $p\equiv 3 \bmod 4$ のときは

$$\begin{aligned}
T(1,p) \;=\; & \frac{1}{2^7\cdot 3^2\cdot 5}(p^2-1)+\frac{1}{2^6\cdot 3}B_{2,\chi} \\
& +\frac{1}{2^5}\left(1-\left(\frac{2}{p}\right)\right)h(\sqrt{-p})+\frac{1}{2^4}h(\sqrt{-2p})+\frac{1}{2^3\cdot 3}h(\sqrt{-3p}) \\
& +\frac{1}{2^6}(p+1)+\frac{1}{2^4}\left(1-\left(\frac{2}{p}\right)\right)+\frac{1}{3^2 2^4}\left(p-\left(\frac{-3}{p}\right)\right)\left(3+\left(\frac{-3}{p}\right)\right) \\
& +\frac{1}{2\cdot 5}\left(1-\left(\frac{p}{5}\right)\right).
\end{aligned}$$

となる。

ここで $h(\sqrt{-d})$ は $\mathbb{Q}(\sqrt{-d})$ の（全整数環の）類数である。また、χ は

$$\chi(x)=\left(\frac{\mathbb{Q}(\sqrt{p})}{x}\right)$$

となるディリクレ指標であり、この導手 を f とするとき、$B_{n,\chi}$ は一般ベルヌーイ数で

$$\sum_{a=1}^{f} \frac{\chi(a)e^{at}}{e^{ft}-1} = \sum_{n=1}^{\infty} \frac{B_{n,\chi}}{n!}t^n$$

で定義される。

Theorem 5.5 ([6]). 類数 $H(1,p)$ は、$p = 2, 3, 5$ については $H(1,2) = H(1,3) = H(1,5) = 1$ であり、$p \geq 7$ については

$$\begin{aligned} H(1,p) &= \frac{1}{2^6 \cdot 3^2 \cdot 5}(p^2-1) + \frac{1}{2^3 3^2}(3p-1) + \frac{p-3}{2^3 3^2}\left(\frac{-3}{p}\right) \\ &\quad + \frac{1}{5}\left(1-\left(\frac{p}{5}\right)\right) + \frac{1}{2^3}\left(1-\left(\frac{2}{p}\right)\right) \\ &\quad + \begin{cases} \dfrac{5(p-1)}{2^5 3} + \dfrac{1}{2^2 3}\left(1-\left(\dfrac{-3}{p}\right)\right) & \textit{if } p \equiv 1 \bmod 4, \\ \dfrac{p+1}{2^5} & \textit{if } p \equiv 3 \bmod 4. \end{cases} \end{aligned}$$

となる。

数値例は以下の通り。

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
H	1	1	1	1	1	2	2	2	2	3	3	5	4	5	4
T	1	1	1	1	1	2	2	2	2	3	3	5	4	5	4

p	53	59	61	67	71	73	79	83	89	97	101	103	107
H	6	5	8	8	6	10	9	8	10	14	12	13	11
T	6	5	8	8	6	10	9	8	10	14	12	13	11

p	109	113	127	131	137	139	149	151	157	163	167
H	16	14	17	14	18	19	20	21	26	24	20
T	16	14	17	14	18	19	20	21	26	24	19

p	173	179	181	191	193	197	199	211	223	227	229
H	25	22	31	24	34	30	31	34	37	32	43
T	24	22	31	24	34	29	31	34	36	30	43

p	233	239	241	251	257	263	269	271	277	281
H	38	34	46	37	44	40	47	49	57	50
T	37	33	46	36	42	38	45	48	56	49

以上の表からわかるとおり、$p < 167$ ならば $H = T$ である。ちなみに -163 は類数が 1 の虚 2 次体の（絶対値が）最大の判別式である。

伊吹山知義 (TOMOYOSHI IBUKIYAMA) 大阪大学 (OSAKA UNIVERSITY)

REFERENCES

[1] T. Asai, The class number of positive definite quadratic forms, Japan J. Math. **3** (1977), 239–296.

[2] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ. Hamburg **14**(1941), 197–272.

[3] M. Deuring, Die Anzahl der Typen von Maximalordnungen einer definiten Quaternionenalgebra mit primer Grundzahl. Jber. Deutsch. Math. Verein. **54** (1950), 24–41.

[4] M. Eichler, Über die Idealklassenzahl total definiter Quaternionenalgebren, Math. Z. **43** (1938), 102–109.

[5] M. Eichler, Zur Zahlentheorie der Quaternionen-Algebren. J. Reine Angew. Math. **195**(1955, 127–151.

[6] K. Hashimoto and T. Ibukiyama, On class numbers of positive definite binary quaternion hermitian forms (I) J. Fac. Sci. Univ. Tokyo Sect. IA**27**(1980), 549–601; (II) ibid. **28** (1982), 695–699; (III) ibid **30**(1983), 393–401..

[7] T. Ibukiyama, Quinary lattices and binary quaternion hermitian lattices, to appear in Tohoku Math. J.

[8] T. Ibukiyama, Type numbers of quaternion hermitian forma and supersingular abelian varieties, to appear in Osaka J. Math.

[9] T. Ibukiyama, T. Katsura and F. Oort, Supersingular curves of genus two and class numbers, Compositio Math. **57**(1986), 127–152.

[10] T. Ibukiyama and T. Katsura, On the field of definition of supersingular polarized abelian varieties and type numbers, Composition Math. **91**(1994), 37–46.

[11] T. Katsura and F. Oort, Supersingular curves of genus two and class numbers, Compositio Math. **57**(1987), 107–167.

[12] K. Z. Li and F. Oort, Moduli of supersingular abelian varieties. Lecture Notes in Math. **1680** Springer-Verlag, Berlin, (1998), iv+116 pp.

[13] M. Peters, Ternäre quadratische Formen und Quaternionenalgebra, Acta. Arith/ **15**(1968/69). 329–365.

[14] G. Shimura, Arithmetic of alternating forms and quaternion hermitian forms. J. Math. Soc. Japan **15** (1963), 33–65

DEPARTMENT OF MATHEMATICS, GRADUATE SCHOOL OF MATHEMATICS, OSAKA UNIVERSITY, MACHIKANEYAMA 1-1, TOYONAKA,OSAKA, 560-0043 JAPAN

E-mail address: ibukiyam@math.sci.osaka-u.ac.jp